Computerized Systems in Drug Establishments (2/83)

FEBRUARY, 1983

National Center for Drugs and Biologics
and
Executive Director of Regional Operations

REFERENCE MATERIALS AND TRAINING AIDS FOR INVESTIGATORS

U.S. DEPT. OF HEALTH AND HUMAN SERVICES
PUBLIC HEALTH SERVICE
FOOD AND DRUG ADMINISTRATION

Division of Drug Quality Compliance (HFN-320)
Associate Director for Compliance
Office of Drugs
National Center for Drugs and Biologics

and

Division of Field Investigations (HFO-500)
Associate Director for Field Support
Executive Director of Regional Operations

I. INTRODUCTION

Computers are being used in increasing numbers in the pharmaceutical industry. As microprocessors become more powerful, reliable, and less expensive we can expect the proliferation of this technology, with increasing use by even very small pharmaceutical establishments. Computer systems are used in a wide variety of ways in a pharmaceutical establishment, such as, maintenance of quarantine systems for drug components, control of significant steps in manufacturing the dosage form, control of laboratory functions, management of warehousing and distribution activities. Computer systems may control one or more of these phases, either singly or as part of a highly automated integrated complex.
The purpose of this guide is to provide the field investigator with a framework upon which to build an inspection of drug establishments which utilize computer systems. This document is not intended to spell out how to conduct a CGMP drug inspection or set forth reporting requirements, but rather what aspects of computerized systems to address during such inspections and suggestions on how to address the systems.

This guide discusses some potential problem areas in application of computer systems, provides inspectional guidance, and includes a glossary of terms the investigator should be aware of prior to performing the inspection. Questions and suggestions concerning this guide should be directed to the Manufacturing Standards and Industry Liaison Branch, Division of Drug Quality Compliance (HFN-323), 443-5307; or the Investigations and Engineering Branch, Division of Field Investigations (HFO-520), 443-3276.

II. OVERVIEW

When a computer system is first encountered in a drug establishment, it may be useful for inspectional purposes to begin with a broad overview of the system(s). Determine exactly what processes and functions are under computer

control or monitoring and which are not. Computer involvement may be much more limited than it may initially appear. For example, computer application may be limited to control of a sterilization cycle in a single autoclave, or maintenance of distribution records.

For each drug process under computer control determine the general system loop (sensors, central processor, activator). For example, the general system loop for a steam autoclave under computer control could consist of temperature/pressure sensors connected to a microprocessor which transmits commands to steam/vacuum control valves.

The overview should enable the investigator to identify those computer controlled processes which are most critical to drug product quality. These are the systems which, of course, merit closer inspection.

III. HARDWARE

For each significant computerized system, it may be helpful to prepare or oed schematic drawing of the attendant hardware. The drawing need only include major input devices, output devices, signal converters, central processing unit, distribution systems, significant peripheral devices and how they are linked. Figure 1 is an example of such a drawing.

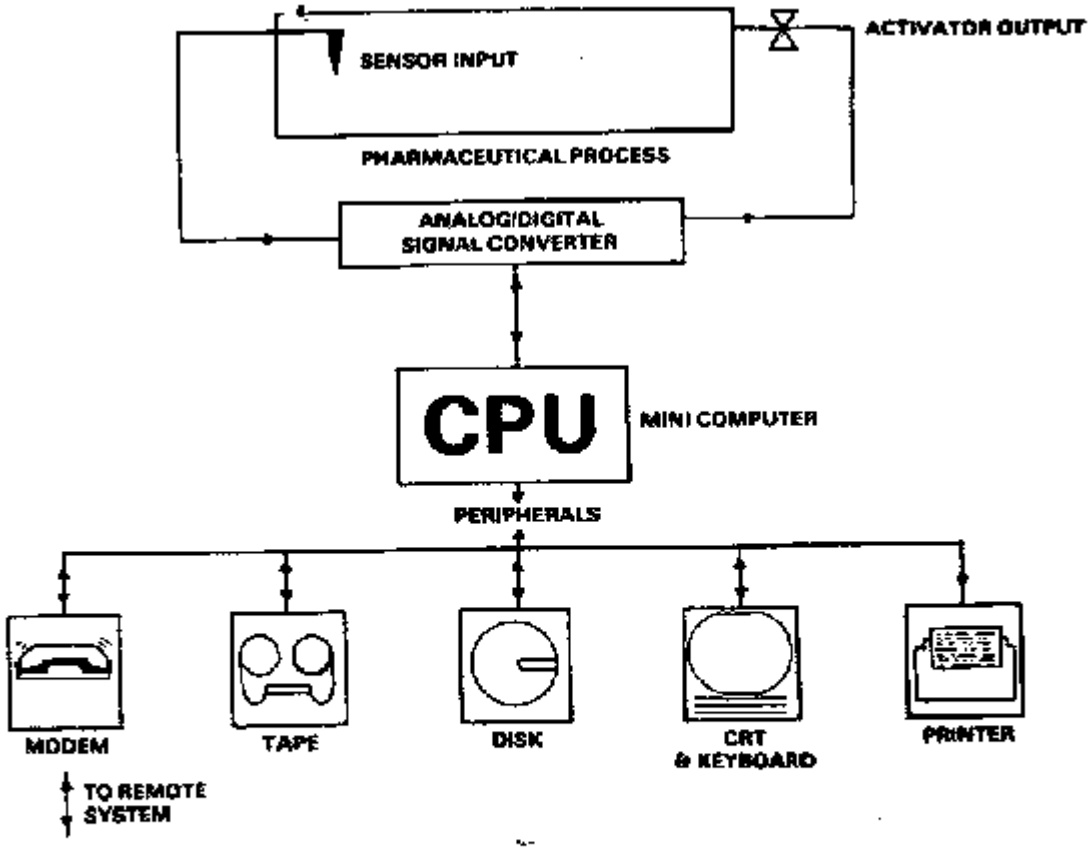

FIGURE 1. EXAMPLE OF COMPUTER SYSTEM SCHEMATIC

Hardware Suppliers. During the inspection identify the manufacturers/suppliers of important computer hardware, including the make and model designations where possible. Hardware to identify this way includes CPUs, disk/tape devices, CRTs, printers, and signal converters. Proper identification of hardware will enable further follow-up at computer vendors should that be needed.

A. Types

1. Input Devices. Equipment which translates external information into electrical pulses which the computer can understand. Examples are thermocouples, flow meters, load cells, pH meters, pressure gauges, control panels, and operator keyboards. Examples of functions are:
   a) Thermocouple provides temperature input for calculation of F value in a sterilizer.
   b) Flow meter provides volume of liquid component going into a mixing tank.
   c) Operator keyboard used to enter autoclave load pattern number.
2. Output Devices. Equipment which receives electrical pulses from the computer and either

causes an action to occur, generally in controlling the manufacturing process, or passively records data. Examples are valves, switches, motors, solenoids, cathode ray tubes (CRTs), printers, and alarms. Examples of functions are:

a) Solenoid activates the impeller of a mixer.
b) Valve controls the amount of steam delivered to a sterilizer.
c) Printer records significant events during sterilization process.
d) Alarm (buzzer, bell, light, etc.) sounds when temperature in a holding tank drops below desired temperature.

Most active output devices will be in proximity to the drug processing equipment under control, but not necessarily close to the CPU. Passive output devices, however, may well be remote from the process or the CPU.

3. Signal Converters. Many input and output devices operate by issuing/receiving electrical signals which are in analog form. These analog signals must be converted to digital signals for use by the computer; conversely, digital signals from the computer must be converted into analog signals for use by analog devices. To accomplish this, signal converter devices are used.
4. Central Processing Unit (CPU). This is the controller containing the logic circuitry of a computer system which conducts electronic switching. Logic circuits consist of three basic sections - memory, arithmetic, and control. The CPU receives electrical pulses from input devices and can send electrical pulses to output devices. It operates from input or memory instructions. Examples and functions are:

a) Programmable controllers can be used for relays, timers and counters.
b) Microprocessors can be used for controlling a steam valve, maintaining pH, etc. They consist of a single integrated circuit on a chip. This is the logic circuit of a microcomputer and microprocessors are often the same as a microcomputer.
c) Microcomputers and minicomputers can be used to control a sterilization cycle, keep records, run test programs, perform lab data analysis, etc.
d) Mainframe computers are usually used to coordinate an entire plant, such as environment, production, records, and inventory.

The distinction between CPUs is becoming less apparent with miniaturization of parts, CPUs are generally ranked by size from "large" mainframes to desk top microcomputers.

5. Distribution System. The interconnection of two or more computers. Also known as distributed processing. Generally, each computer is capable of independent operation but is connected to other computers in order to have a back-up system, to receive operating orders and to relay what is executed by other computers. Typical of such

distribution systems is the linkage of smaller or less powerful units to larger or more powerful units. For example, a minicomputer may command and communicate with several microcomputers. A large CPU may also act as a "host" for one or more other CPU's. When such systems are encountered during an inspection, it is important to know the configuration of the system and exactly what commands and information can be relayed amongst the computers. Figure 2 contains examples of distributed control.

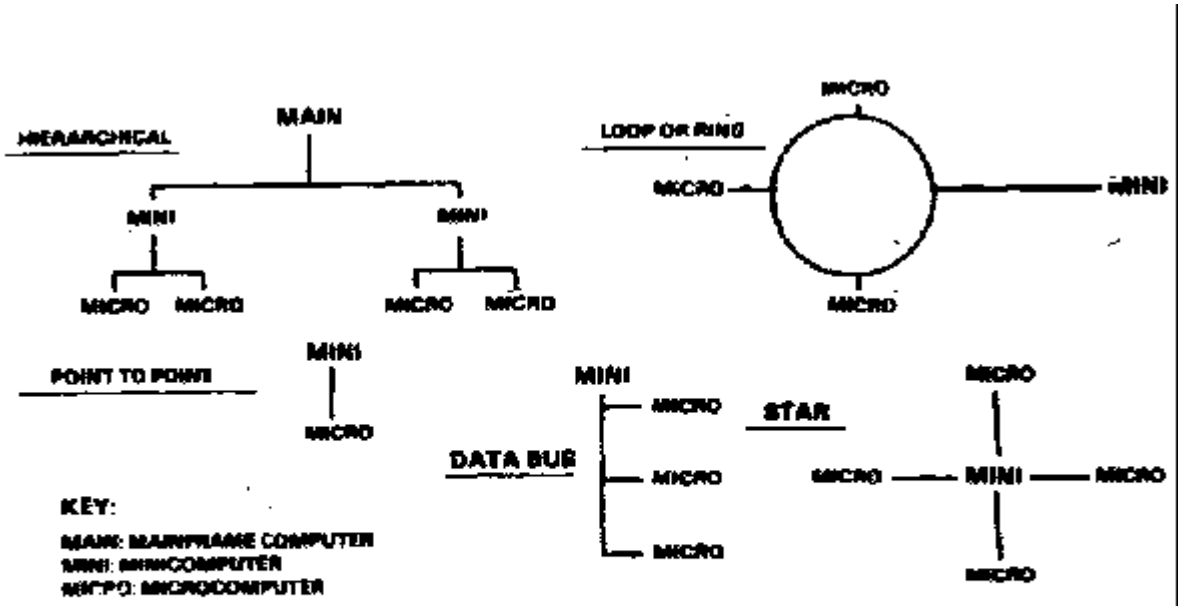

FIGURE 2. EXAMPLE OF DISTRIBUTED COMPUTER CONTROL CONFIGURATIONS

Networks are generally extensions of distributed processing. They typically consist of connections between complete computer systems which are geographically distant. Potentially, pharmaceutical companies could have international networks by using modems and satellites.

6. Peripheral Devices. All computer associated devices external to the CPU can be considered peripheral devices. This includes the previously discussed input and output devices. Many peripheral devices can be both input and output, they are commonly known as I/O devices. These include CRTs, printers, keyboards, disk drives, modems, and tape drives.

B. Key Points

1. Location. Three potential problems have been identified with location of CPUs and peripheral devices. These are:
   a) Hostile Environments. Environmental extremes

of temperature, humidity, static, dust, power feed line voltage fluctuations, and electromagnetic interference should be avoided. Such conditions may be common in certain pharmaceutical operations and the investigator should be alert to locating sensitive hardware in such areas. Environmental safeguards maybe necessary to ensure proper operation. There are numerous items on the market (such as line voltage monitors/controllers and anti-static floor mats) designated to obviate such problems. Physical security is also a consideration in protecting computer hardware from damage; for example, books and bottles of reagents should not be stored on top of microprocessors. Likewise eating, drinking and smoking should be restricted in rooms housing mainframes.

b) Excessive Distances between CPU and Peripheral Devices. Excessively long low voltage electrical lines from input devices to the CPU are vulnerable to electromagnetic interference. This may result in inaccurate or distorted input data to the computer. Therefore, peripheral devices located as near to the CPU as practical and the lines should be shielded from such sources of electromagnetic interference as electrical power lines, motors, and fluorescent lighting fixtures. In a particularly "noisy" electronic environment this problem might be solved by the use of fiber optic lines to convey digital signals.

c) Proximity of Input Devices to Drug Processing. Input devices which are remote from (out of visual range of) the drug processing equipment are sometimes met with poor employee acceptance.

2. Signal Conversion. Proper analog/digital signal conversion is important if the computer system is to function accurately. Poor signal conversion can cause interface problems. For example, an input sensor may be feeding an accurate analog reading to a signal converter, but a faulty signal converter may be sending the CPU an inappropriate digital signal.

3. I/O Device Operation. The accuracy and performance of these devices are vital to the proper operation of the computer system. Improper inputs from thermocouples, pressure gauges, etc., can compromise the most sophisticated microprocessor controlled sterilizer. These sensors should be systematically calibrated and checked for accurate signal outputs.

4. Command Over-rides. In distributed systems it is important to know how errors and command over-rides at one computer are related to operations at another computer in the system. For example, if each of three interconnected microcomputers runs one of the three sterilizers, can a command entered at one unit inadvertently alter the sterilization cycle of a sterilizer under the control of a different microcomputer on

the line? Can output data from one unit be incorrectly processed by another unit? The limits on information and command for distributed system should be clearly established by the firm.

5. Maintenance. Computer systems usually require a minimum of complex maintenance. Electronic circuit boards, for example, are usually easily replaced and cleaning may be limited to dust removal. Diagnostic software is usually available from the vendor to check computer performance and isolate defective integrated circuits. Maintenance procedures should be stated in the firm's standard operating procedures. The availability of spare parts and access to qualified service personnel are important to the operation of the maintenance program.

C. Validation of Hardware

The suitability of computer hardware for the tasks assigned to pharmaceutical production must be demonstrated through appropriate tests and challenges. The depth and scope of hardware validation will depend upon the complexity of the system and its potential affect on drug quality.

The validation program need not be elaborate but should be sufficient to support a high degree of confidence that the system will consistently do what it is supposed to do. In considering hardware validation the following points should be addressed:

1. Does the capacity of the hardware match its assigned function? For example, in a firm using a computer system to maintain its labeling text, including foreign language labeling, do the CRT and printer have the capacity to write foreign language accent marks?
2. Have operational limits been identified and considered in establishing production procedures? For example, a computer's memory and connector input ports may limit the number of thermocouples a computer can monitor. These limits should be identified in the firm's standard operating procedures.
3. Have test conditions simulated "worst case" production conditions? A computer may function well under minimal production stress (as in vendor's controlled environment) but falter under high stresses of equipment speed, data input overload or frequent or continuous multi-shift use (and a harsh environment). Therefore, it is insufficient to test computer hardware for proper operation during a one hour interval, when the system will be called upon in worst case conditions to run continuously for 14 days at a time. Some firms may test the circuits of a computer by "feeding" it electrical signals from a signal simulator. The simulator sends out voltages which are designed to correspond to voltages normally transmitted by input devices. When simulators are connected to the computer, the program should be executed as if the emulated input devices were actually connected. These signal simulators can be useful tools for

validation; however, they may not pose worse case conditions and their accuracy in mimicking input device performance should be established. In addition, validation runs should be accomplished on line using actual input devices. Signal simulators can also be used to train employees on computer operations without actually using production equipment.

4. Have hardware tests been repeated enough times to assure a reasonable measure of reproducibility and consistency? In general, at least three test runs should be made to cover different operating conditions. If test results are widely divergent they may indicate an out of control state.
5. Has the validation program been thoroughly documented? Documentation should include a validation protocol and test results which are specific and meaningful in relation to the attribute being tested. For example, if a printer's reliability is being tested it would be insuess the results merely as "passes," in the absence of other qualifying data such as printing speeds, duration of printing, and the number of input feeds to the printing devices.
6. Are systems in place to initiate revalidation when significant changes are made? Revalidation is indicated, for example, when a major piece of equipment such a circuit board or an entire CPU is replaced. In some instances identical hardware replacements may adequately be tested by the use of diagnostic programs available from the vendor. In other cases, as when different models of hardware are introduced, more extensive testing under worst case production conditions, is indicated.

Much of the hardware validation may be performed by the computer vendor. However, the ultimate responsibility for suitability of equipment used in drug processing rests with the pharmaceutical manufacturer. Hardware validation data and protocols should be kept at the drug manufacturer's facility. When validation information is produced by an outside firm, such as the computer vendor, the records maintained by the drug establishment need not be all inclusive of voluminous test data; however, such records should be reasonably complete (including general results and protocols) to allow the drug manufacturer to assess the adequacy of the validation. A mere certification of suitability from the vendor, for example, is inadequate.

IV. SOFTWARE

Software is the term used to describe the total set of programs used by a computer. These programs exist at different language levels, generally the higher the level, the closer the text is to human language. These levels are set forth below. During the inspection identify key computer programs used by the firm. Of particular importance are those programs which control and document dosage form production and laboratory testing. Usually a firm can readily list the names of such programs on a CRT

display or in hard copy. Such a list is sometimes called a menu or main menu.

A. Levels

1. Machine Language. This laof coded instructions, represented by binary numbers, which are executed directly by the computer.
2. Assembly Language. Instructions are represented by alphanumeric abbreviations. These programs must be converted into machine language, sometimes called "object programs," before they can be executed. Programs which translate assembly programs to object programs are called assemblers. Different computers have different assembly languages. Computer manufacturers usually provide the assembler program.
3. High Level Language. This language is characterized by a vocabulary of English words and mathematical symbols. These are source programs which must be translated by a compiler or interpreter into an object program. High level languages generally operate the same on any computer which accepts the language although there may be different versions of the same language. Examples are FORTRAN, BASIC, and COBOL.
4. Application Language. This is generally based on a high level language but modified for a specific industry application and uses the vocabulary of that industry. Examples are AUTRAN (Control Data Corporation) and Foxboro Process Basic.

B. Software Identification

For the key computer programs used by a firm, the following items should be identified:

1. Language. High level or application name should be determined (or machine or assembly language).
2. Name. Programs are usually named with some relationship to what they do, i.e. Production Initiation, Batch History Transfer or Alarms.
3. Function. Determine what the purpose of the program is, i.e., start production, record and print alarms, or calculate F.
4. Input. Determine inputs, such as thermocouple signals, timer, or analytical test results.
5. Output. Determine what outputs the program generates. These may be a form of mechanical action (valve actuation) or recorded data (generation of batch records).
6. Fixed Setpoint. This is the desired value of a process variable which cannot be changed by the operator during execution. Determine major fixed setpoints, such as desired time/temperature curve, desired pH, etc. Time may also be used as a set point to stop the process to allow the operator to interact with the processing.
7. Variable Set point. This is the desired value of a process variable which may change from run to run and must usually be entered by the operator. For example, entering one of several sterilizer load patterns into a sterilization computer process.
8. Edits. A program may be written in such a manner as to reject or alter certain input or output

information which does not conform to some pre-determined criterion or otherwise fall within certain pre-established limits. This is an edit and it can be a useful way of minimizing errors; for example, if a certain piece of input data must consist of a four character number, program edits can be used to reject erroneous entry of a five character number or four characters comprised of both numbers and letters. On the other hand, edits can also be used to falsify information and give the erroneous impression that a process is under control; for example, a program output edit may add a spurious "correction" factor to F values which fall outside of the pre-established limits, thus turning an unacceptable value into an ue. It is, therefore, important to attempt to identify such significant program edits during the inspection, whenever possible. Sometimes such edits can manifest themselves in unusually consistent input/output information.

9. Input manipulation. Determine how a program is set up to handle input data. For example, determine what equations are used as the basis for calculations in a program. When a process is under computer control determine, in simplified form such as a flow chart, how input is handled to accomplish the various steps in the process. This does not mean that a copy of the computer program itself needs to be reviewed. However, before computerized control can be applied to a pharmaceutical process there usually needs to be some source document, written in English, setting forth in logical steps what needs to be done; it would be useful to review such a document in evaluating the adequacy of conversion from manual to computerized processing.
10. Program Over-rides. A program may be such that the sequence of program events or program edits can be over-ridden by the operator. For example, a process controlling program may cause a mixer to stop when the mixer's contents reach a predetermined temperature. The program may prevent the mixer from resuming activity until the temperature has dropped back to the established point. However, the same program may allow an operator to over-ride the stop and reactivate the mixer even at a temperature which exceeds the program limit. It is therefore important to know what over-rides are allowed, and if they conflict with the firm's SOP.

C. Key Points

1. Software Development. During the inspection determine if the computer programs used by the firm have been purchased as "canned" from outside vendors, developed within the firm, prepared on a customized basis by a software producer, or some combination of these sourams are highly specialized and may be licensed to pharmaceutical establishments. If the programs used by the firm are purchased or developed by outside vendors determine which firms prepared the programs.

In some cases "canned" or customized programs may contain segments (such as complex algorithms) which are proprietary to their authors and which cannot normally be readily retrieved in program code without executing complex code breaking schemes. In these cases the buyer must accept on faith that the software will perform properly. If the drug manufacturer is using such a program to control or monitor a significant process, determine what steps the firm has taken to assure itself that such program blind spots do not compromise the program performance.

Where drug firms develop their own application programs, review the firm's documentation of the approval process. This approval process should be addressed in the firm's SOP. It may be useful to review the firm's source (English) documents which formed the basis of the programs.

2. Software Security. Determine how the firm prevents unauthorized program changes and how data are secure from alteration, inadvertent erasures, or loss (21 CFR 211.68). Some computers can only be operated in a programming mode when two keys are used to unlock an appropriate device. When this security method is used, determine how use of keys is restricted. Another way of achieving program security is the use of ROM (read only memory), PROM (programmable read only memory), or EPROM (erasable programmable read only memory) modules within the computer to "permanently" store programs. Usually, specialized equipment separate from the computer is needed to change an EPROM or establish a program in PROM so that changes would not be made by the operator. A program in EPROM is erase the module (which has a quartz window) to ultraviolet light. In these cases a program is secure to the extent it can't be over-ridden by the operator. Determine who in the firm has the ability and/or is authorized to write, alter or have access to programs. The firm's security procedures should be in writing. Security should also extend to devices used to store programs, such as tapes, disks and magnetic strip cards. Determine if accountability is maintained for these devices and if access to them is limited. For instance, magnetic strip cards containing a program to run a sterilization cycle may be kept in a locked cabinet and issued to operators on a charge-out basis with return of the card immediately after it is used.

D. Validation of Software

It is vital that a firm have assurance that computer programs, especially those that control manufacturing processing, will consistently perform as they are supposed to within pre-established operational limits. Determine who conducted software validation and how key programs were tested. In considering software validation the following points should be addressed:

1. Does the program match the assigned operational function? For example, if a program is assigned to generate batch records then it should account for the maximum number of different lots of each

component that might be used in the formulation. Consider what might happen when three lots of a component are used with a program designed to record lot designations and quantities for up to two different lots of each component. The first lot may be accurately recorded, but the next two lots might be recorded as a single quantity having the second lot designation; the resultant computer generated record therefore would fail to show the use of three different lots and the quantities of each of the second and third lots going into the mixture.

2. Have test conditions simulated "worst case" production limits? A program should be tested, for example, under the most challenging conditions of process speed, data volume and frequency. Date should be considered in this aspect of validation. For example, the number of characters allowed for a lot number should be large enough to accommodate the longest lot number system that will be used.
3. Have tests been repeated enough times to assure consistent reliable results? Divergent results from replicate data entries may signify a program bug. In general, at least three separate runs should be made.
4. Has the software validation been thoroughly documented? Documentation should include a testing protocol and test results which are meaningful and specific to the attribute being tested; individuals who reviewed and approved the validation should be identified in the documentation.
5. Are systems in place to initiate revalidation when program changes are made? If process parameters such as time/temperature, sequence of program steps, or data editing/handling are changed then revalidation is indicated.

Although much of the software validation may be accomplished by outside firms, such as computer or software vendors, the ultimate responsibility for program suitability rests with the pharmaceutical manufacturer. Records of software validation should be maintained by the drug establishment, although when conducted by outside experts such records need not be voluminous but rather complete enough (including protocols and general results) to allow the drug manufacturer to assess the adequacy of the validation. Mere vendor certification of software suitability is inadequate. Signal simulators many be used in software validation. These are discussed in point No. 3 of Validation of Hardware.

V. COMPUTERIZED OPERATIONS

A. Networks

If the firm is on a computer network it is important to know: (1) what output, such as batch production records, is sent to other parts of the network; (2) what kinds of input (instructions, programs) are received; (3) the identity and location fo establishments which interact with the firm; (4)the extent and nature of monitoring and controlling activities exercised by remote on-net establishments;

and (5) what security measures are used to prevent unauthorized entry into the network and possible drug process sabotage.

It is possible under a computer network for manufacturing operations conducted in one part of the country to be documented in batch records on a real-time basis in some other part of the country. Such records must be immediately retrievable from the computer network at the establishment where the activity took place (21 CFR 211.180).

B. Manual Back-up Systems

Functions controlled by computer systems can generally also be controlled by parallel manual back-up systems. During the inspection determine what functions can be manually controlled and identify manual back-up devices. Process controls are particularly important. Determine the interaction of manual and computerized process controls and the degree to which manual intervention can over-ride or defeat the computerized process. The firm's SOP should describe what manual over-rides are allowed, who may execute them, how and under what circumstances. Determine if and how manual interventions are documented; a separate log may be kept of such interventions. The computer system may be such that it detects, reacts to and automatically records manual interventions and this should be addressed during the inspection.

C. Input/Output Checks

Section 211.68 of the CGMP regulations requires that input to and output from the computer system be checked for accuracy. While this does not mean that every bit of input and output need be checked it does mean that checking must be sufficient to provide a high degree of assurance that input and output are, in fact, accurate. In this regard theome reasonable judgment as to the extent and frequency of checking based upon a variety of factors such as the complexity of the computer systems. The right kinds of input edits, for example, could mitigate the need for extensive checks.

During the inspection determine the degree and nature of input/output checks and the use of edits and other built-in audits.

Input/output error handling has been a problem in computer systems. Determine the firm's error handling procedures including documentation, error verification, correction verification, and allowed error over-rides including documentation of over-rides.

As an illustration of inadequate input/output checks and error handling consider the situation of a firm which uses a computer system to maintain and revise labeling text. Master labeling is recorded on a disk and when a change is to be made the operator calls up a copy of the text from the master disk onto a CRT. The copy is then revised at the CRT, printed on paper and electronically printed onto another disk for storage until the paper copy is proofread and approved; once the paper copy is approved, the text on the temporary storage disk is transferred to the master disk replacing the previous text. As an example, the operator calls up a label to change the directions for use section, correctly makes the change but accidentally erases the quantity of content statement

that read 100 ml. The operator "corrects" this error by re-entering what was believed to be the correct statement but what, in fact, was "150 ml." The proof-readers do not detect this error because their standard operating procedure is to proof only those portions of the labeling-in this case directions for use-which were supposed to be changed (a case of inadequate output check). In addition, the operator does not document the error or the "correction" and the "correction" is not verified. This would probably result product. Section 211.68 of the CGMP regulations also requires maintenance of accurate back-up files of input data which are secure from alteration, loss or inadvertent erasure. These back-up files need not be on paper, however. They may, for instance, consist of duplicate tapes, disks or microfilm. During the inspection determine if the firm has such a back-up system, the form of such a system, and how it is protected. If a back up file is printed on thermal paper note if older files have faded. (It has been reported that the printing on thermal paper has a tendency to fade with time.)

D. Process Documentation

Most computer systems are capable of generating accurate and detailed documentation of the drug process under computer control. What is important is that records within the scope of the CGMP regulations, which happen to be in computerized form, do contain all of the information required. For example, if batch production records are generated by computer determine if they contain all of the information required to be in batch records.

E. Monitoring of Computerized Operations

Determine the degree to which the firm's personnel monitor computerized operations. Is such monitoring continuous or periodic? What functions are monitored? For example, a firm's computer system may be used to maintain the pH in a reaction vessel, but if the firm does not sufficiently monitor the system they may fail to detect a hardware problem which could allow the pH to be out of tolerance. During the inspection, where possible, spot-check computer operations such as:

1. Calculations; compare manual calculations of input data with the automated calculations or ask the firm to process a given set of input values and compare automated results against known results.
2. Input recording; compare sensor indications with what the computer indicates, for example. As mentioned previously, some analog signals may be incorrectly converted to digital signals and built-in programming edits may alter input data. For example, a thermocouple indicating 80øC may read out on a CRT as 100øC or any other temperature if the signal con malfunctioning.
3. Component quarantine control; for example, check the actual warehouse location of a particular lot against its location as reported by computer. If the computer indicates that a particular lot has passed a certain number of laboratory tests then the laboratory records may be checked to confirm the computer information.
4. Timekeeping; where computers are reporting events

and controlling a process in real time, spot-check the time accuracy against a separate time piece; accurate timekeeping is especially important where time is a determinative or limiting factor in a process such as sterilization. It should be noted that some computer systems run on a 12 hour clock whereas others run on a 24 hour clock.

5. Automated cleaning in-place; determine the procedure used, how the firm assures adequacy of cleaning, and residue elimination.
6. Tailings accountability; where batches are produced back to back on a continuous basis under computer control are batch tailings accounted for in subsequent handling and formulation? For example, at the conclusion of a run the computer's memory may be downloaded and the controlling program reset. At an initial step the computer may call for a programmed quantity of material to be added to a hopper; the amount to be added can be based upon the tare weight of an empty hopper. However, if the hopper is not, in fact, empty but contains tailings of a prior run the result may be a hopper with more material than called for in the batch formulation; thus, there may be errors of yield reconciliation or batch formulation. During the inspection determine what limits if any the firm places on tailings.

F. Alarms

A typical computer system er of built-in alarms to alert personnel to some out-of-limits situation or malfunction. Determine what functions are linked to alarms. For example, alarms may be linked to power supply devices, feedback signals to confirm execution of commands, and pharmaceutical process conditions such as empty or overflowing tanks. Determine the alarm thresholds for critical process conditions and whether or not such thresholds can be changed by the operator. For example, if the temperature of water in a water for injection system is linked to an alarm which sounds when the temperature drops below 80øC, can the operator change the threshold to 75øC?

Determine how the firm responds when an alarm is activated. This should be covered in the firm's standard operating procedures.

Determine the types of alarms (lights, buzzers, whistles, etc.) and how the firm assures their proper performance. Are they tested periodically and equipped with in-line monitoring lights to show they are ready?

Because an activated alarm may signal a significant out of control situation it is important that such alarm activations are documented. Determine how alarm soundings are documented-in batch records, in separate logs or automatic electronic recording, for instance. Can all alarm conditions be displayed simultaneously or must they be displayed and responded to consecutively? If an employee is monitoring a CRT display covering one phase of the operation will that display alert the employee to an alarm condition at a different phase? If so, how?

G. Shutdown Recovery

How a computer controlled process is handled in the event of computer shutdown (e.g. power failure) is significant and can pose a problem. Shutdown recovery procedures are not uniform in the industry. Some systems, for example, must be restarted from the initial step in the process sequence and memory of what has transpired is lost. Other systems have safeguards whereby memory is retained and the process is resumed at the point Determine the disposition of the computer's memory content (program and data) upon computer shutdown.

Determine the firm's shutdown recovery procedure and whether or not, in the event of computer failure, the process is brought into a "safe" condition to protect the product. Determine such safeguards and how they are implemented. Where is the point of restart in the cycle--at the initial step, a random step or the point of shutdown? Look for the inappropriate duplication of steps in the resumption of the process.

The time it takes to resume a computerized process or switch to manual processing can be critical, especially where failure to maintain process conditions for a set time (e.g. pH control for antibiotic fermentation) compromises product integrity. Therefore, note recovery time for delay-sensitive processes and investigate instances where excessive delays compromise product quality or where established time limits (21 CFR 211.111) are exceeded.

Many systems have the ability to be run manually in the event of computer shutdown. It is important that such back-up manual systems provide adequate process control and documentation. Determine if back-up manual controls (valves, gates, etc.) are sufficient to operate the process and if employees are familiar with their operation. Records of manual operations may be less detailed, incomplete, and prone to error, compared to computerized documentation, especially when they are seldom exercised. Therefore, determine how manual operations are documented and if the information recorded manually conforms with CGMP requirements.

VI. CGMP GUIDANCE

A. Hardware

In general, the hardware of a computer system is considered to be equipment within the meaning of the CGMP regulations. Therefore those sections of the regulations which address equipment apply to hardware. For example, the following apply:

1. 21 CFR 211.63 repment be suitably located to facilitate operations for the equipment's intended use.
2. 21 CFR 211.67 requires a maintenance program for equipment.
3. 21 CFR 211.68(a) states that computers may be used and requires a calibration program.

B. Software

In general, software is regarded as records or standard operating procedures (instructions) within the meaning of the CGMP regulations and the corresponding sections of the CGMP regulations apply, for example:

1. Record Controls. 21 CFR 211.68(b) requires programs to ensure accuracy and security of computer inputs, outputs, and data.

2. Record Access. 21 CFR 211.180(c) states that records required by the regulations shall be available as part of an authorized inspection at the establishment for inspection and are subject to reproduction. Computer records retrievable from a remote location are acceptable.
   In considering the copying of electronic records however, the act of copying must be reasonable, as the word reasonable is used in the FD& C Act to limit how we may conduct inspections. In some cases it may be reasonable to copy a disk or tape whereas in other cases it might not, particularly where we would have to physically remove the disk or tape from the establishment in order to copy it. (Consider the analogy of removing an entire file cabinet so that we can copy five pieces of paper.) We believe that, rather than copy an entire disk or tape ourselves, it is preferable to have the firm generate hard copies of only those portions of the disk or tape which we need to document.
3. Record Medium. 21 CFR 211.180(d) states that retained records may be originals or true copies and, when necessary, ocopying equipment shall be available. This concept applies to magnetic tape and disks.
4. Record Retention. 21 CFR 211.180(a) states record retention requirements. They are the same for electronic media and paper.
5. Computer Programs. FD& C Act. Section 704(a), for prescription drug products, would allow inspectional access to computer programs if such inspection is performed within the constraint of being reasonable.
   There are several factors which must be considered on a case by case basis in determining what is reasonable in accessing a firm's computer. For example, the effect on drug production is a factor; specifically, if the process of running a program disrupts drug production in an adverse manner then that would be unreasonable. Another factor is whether or not our manipulations give us access to unauthorized information; the data we may be searching with a program may contain some information we are not entitled to review such as financial data. Consider also that some computer programs are protected by copyright and carefully licensed to software users; thus, we would not be able to copy and use such programs without prior approval of their owners.
6. Record Review. 21 CFR 211.180(e) states that where appropriate records associated with every batch shall be reviewed as part of a periodic review of quality standards. It is acceptable for a firm to conduct part of the review by running a computer program which culls out analytical data from each batch and conducts trend analysis to determine the need to change product specifications, manufacturing methods, or control prata itself must be meaningful (i.e., specified and relevant to enable an evaluation to be performed). It is not necessary to review each and every bit of information on the

batch record. However, the computerized trend analysis data would constitute only a portion of the data which must be reviewed. A review must also be made of records of complaints, recalls, returned or salvaged products, and investigations of unexpected production discrepancies (e.g., yield reconciliations) and any failures of batches to meet their specifications. This information is usually separate from conventional batch records and so would not necessarily be reviewed by the trend analysis program.

7. QC Record Review. 21 CFR 211.192 requires the quality control unit to review and approve production and control records prior to batch release/distribution. If this record screening review (to check errors and anomalies) is computerized and is at least as comprehensive and accurate as a manual review, then it is acceptable for the QC unit to review a computer generated exception report as part of the batch release. The batch record information required by the regulation must still be retained. It is also important that the accuracy and reliability of the screening program be demonstrated. It is unlikely however, that all production and control records will be computerized; labeling, packaging, and analytical records may still be in manual form and would therefore be manually reviewed.
8. Double Check on Computer. 21 CFR 211.101(d) requires verification by a second person for components added to a batch. A single check automated system is acceptable if it provides at least the same assurance of freedom from errors as a double check. If it does provide the same assurance then we would gain nothing in applying a redundant second check which adds nothing to assuring product quality. The equivalency of an automated single check system to a manual check must be shown, however, and this might not always be possible. For example, let's say 5 kilograms of a coarse white granular component must be added to a mixture. Two individuals checking the operation may check for the component's label accuracy, color and granularity, weight and finally the actual transfer of the material; if there were a mix-up prior to that transfer and a different component, say a white powder, was staged for addition to the batch it is probable that the double check screening would detect the error. On the other hand, a single check computer system might accurately check the component weight and physical transfer but not its granularity or other sign of identification. In this case the automated single check would not be as good as the manual double check.
9. Documentation. 21 CFR 211.188(b) (11) requires that batch production and control records include identification of each person who conducts, supervises or checks each significant step in the process. The intent is to assure that each step was, in fact, performed and that there is some record to show this, from which the history of the lot could be traced. It is quite possible that an

automated system can achieve the same, or higher, level of assurance in which case it may not be necessary to have persons document the performance of each event in a series of unbranched automated events on the production line. For example, let us say an automated/computerized system is designed to perform steps A through Z. If the program is such that every step must be executed properly before step Z is completed then an acceptable means of complying with the regulation would be all of the following: (1) documentation of the program; (2) validation that no step can be missed or poorly executed; and (3) documentation of the initial and final steps. It would not be necessary in this example to document steps B through Y.

10. Reproduction Accuracy. 21 CFR 211.188(a) requires the batch record to contain a reproduction of the master record. The intent is to insure that the batch was, in fact, produced according to the approved formulation, manufacturing instructions and controls. The act of computer transcription can generate errors. The firm should check for such errors or otherwise assure that no errors can occur. During the inspection the investigator can ask to see the original approved, endorsed, master record and compare it to the batch record. The fact that the batch record is a second or third generation copy is not in and of itself objectionable provided it is accurate.
11. NDA Considerations. 21 CFR 314.8 requires that a supplement be submitted for changes in manufacturing/control processes or facilities from those stated in the approved NDA. If a firm has changed from a manual to a computerized system under an NDA, that change should be covered by a supplemental application. If the change gives increased assurance of product quality, then the change can be put into effect before the supplement has been approved. However, such supplements should state the anticipated implementation date (which should be sometime after the submission date) to allow reviewing chemists the lead time needed to determine if the type of change proposed is, in fact, of the kind which may be implemented prior to approval.

GLOSSARY

ADDRESS	A switch pattern which identifies the location of a piece of data or a program step.
ALGORITHM	A systematic procedure or equation designed to lead to the solution of a problem in a finite number of steps.
ALU	Arithmetic Logic Unit; the circuitry within the CPU which performs all arithmetic functions.
ANALOG	Continuous signal having a voltage which corresponds to the monitored value.
APPLICATIONS	Term used to describe software written to perform tasks on a computer.

ASCII	American Standard Code for Information change; a system used to translate keyboard characters into bits.
ASSEMBLER	Program which translates assembly code to executable machine code; e.g. assembly code ADD becomes machine code 04.
ASSEMBLY CODE	Symbolics, a simple language; different computers have different assembly codes.
ASYNCHRONOUS	Term used to describe the exchange of information piece by piece rather than in long segments.
AUXILIARY STORAGE	Storage device other than main storage; disks and tapes.
BASIC	Beginner's All Purpose Symbolic Instruction Code; a high level language.
BATCH PROCESSING	Execution of programs serially with no interactive processing.
BAUD	The rate at which data is received or transmitted in serial: one baud is one bit per second.
BINARY	The base two number system. Permissible digits are 0 and 1.
BIT	Binary Digit; the smallest unit of information in a computer, represented as 0 or 1, off or on for a switch.
BOOT	An initialization program used to set up the computer when it is turned on.
BUFFER	Part of memory used to temporarily hold data for further processing.
BUG	A program error.
BUS	Electrical pathway by which information flows to different devices.
BYTE	A sequence of adjacent bits, usually eight, operated upon as a unit; the lowest addressable unit in a computer.
COMPILER	Program which translates a computer language into executable machine code. A compiler translates an entire program before the program is run by the computer.
CP/M	Control Program for Microcomputers; a registered trademark of Digital Research; an operating system.
CPU	Central processing unit of a computer where the logic circuitry is located; the CPU controls the entire computer; it sends and receives data through input-output channels, retrieves data from memory and conducts all program processes.
CRT TERMINAL	Cathode ray tube; an input/output device.
DATABASE	Collection of data, at least one file, fundamental to a system.
DATA SET	Term synonymous with file.
DIGITAL	Relating to separate and discrete information.
DISK	A circular rotating magnetic storage device. Disks come in different sizes and can be hard or flexible.
DISK DRIVE	A device used to read from or write to a disk or diskette.
DISK OPERATING SYSTEM	DOS, a program which operates a disk drive.
DISKETTE	A floppy disk.

EPROM	Erasable programmable read only memory: switch pattern in circuit can be erased by exposure to ultraviolet light.
FILE	Set of related records treated as a unit, stored on tape or disk; synonymous with data set.
FIRMWARE	A program permanently recorded, e.g., in ROM.
HARD COPY	Output on paper.
HARDWARE	Physical electronic circuitry and associated equipment.
HEXADECIMAL	The base 16 number system. Digits are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, AND F. This is a convenient form in which to examine binary data because it collects 4 binary digits per hexadecimal digit. E.g. Decimal 15 is 1111 in binary and F in hexadecimal.
INTEGRATED CIRCUIT (IC)	Small wafers of silicon etched or printed with extremely small electronic switching circuits; also called CHIPS.
INTERACTIVE PROCESSING	An application in which each entry calls forth a response from a system or program, as in a ticket reservation system.
INTERFACE	A device which permits two or more devices to communicate with each other.
INTERPRETER	A program which translates a high level language into machine code one instruction at a time. Each instruction in the high level language is executed before the next instruction is interpreted.
I/O PORT	Input/output connector.
JOB	Set of data completely defining a unit of work for a computer.
K	Symbol representing two to the tenth power, 1024, usually used to describe amounts of computer memory, and disk storage, in bytes.
LANGUAGE	Any symbolic communication media used to furnish information to a computer. Examples are PL/1, COBOL, BASIC, FORTRAN, AND ASSEMBLY.
LOADER	A program which copies other programs from external to internal storage.
MACHINE CODE	Numerial representations directly executable by a computer; sometimes called machine language.
MAIN STORAGE	Term synonymous with MEMORY.
MAINFRAME	Term used to describe a large computer.
MEGABYTE	1024K Bytes
MEMORY	A non-moving storage device utilizing one of a number of types of electronic circuitry to store information.
MENU	A CRT display listing a number of options. the operator selects one of the options. Sometimes used to denote a list of programs.
MICROCOMPUTER	A small computer (See MICROPROCESSOR).
MICROPROCESSOR	Usually a single integrated circuit on a chip; logic circuitry of a microcomputer; frequently synonymous with a microcomputer. A microprocessor executes encoded instructions to perform arithmetic operations, internal data transfer, and communications with external devices.

MINICOMPUTER	Medium sized computer.
MODEM	Modulator - demodulation, a device which accepts data from a computer, and sends data to a computer, over telephone wires or cables. A half duplex MODEM can only receive or transmit data at one time. A full duplex MODEM can receive and transmit data at the same time.
MULTIPLEXER	A device which takes information from any of several sources and places it on a single line.
NETWORK	A system that ties together several remotely located computers via telecommunications.
OBJECT CODE	Term synonymous with machine code.
OEM	Original Equipment Manufacturer (i.e. maker of computer hardware).
OPERATING SYSTEM	Set of machine language programs that run accessories, perform commands and interpret or translate high level language program (usually written into the ROM).
PARALLEL	Term to describe transmission of data eight bits (one byte) at a time.
PARITY BIT	An extra bit within a byte; used to verify the coded information in the byte itself. The extra bit is either a one or zero so as to make the total number of ones in a byte equal either an odd or even number (odd or even parity).
PERIPHERAL	A general term used to describe an input or output device.
PROGRAM	A collection of logically interrelated statements written in some computer language which, after translation into machine code, performs a predefined task when run on the computer.
PROM	Programmable read only memory; once programmed the switch pattern on a PROM cannot be changed. Special equipment separate form the computer is usually used to "burn in" the switch pattern.
	communication between computers, i.e. physical electrical links, message format, message priorities, etc.
RAM	Random access memory; internal storage device containing volatile information which can be changed; read-write memory. When electrical power is cut off from a RAM IC its memory is lost.
RECORD	Collection of related data treated as a unit.
SERIAL	Term to describe handling of data one bit at a time.
ROM	Read only memory; internal storage device in which information is permanent.
RS-232C	An Electronic Industries Association (EIA) standard for connecting electronic equipment; data is transmitted and received in serial format. This is an interface standard that usually uses a 25 pin connector.
SOFTWARE	Programs executable on a computer. Programs are written in any number of different languages.
SOURCE PROGRAM	High level language program which the operator can read.
STORAGE DEVICE	A unit into which can

	be placed, retained and retrieved.
SYNTAX	Required grammar or structure of a language.
SYSTEM	Term can refer to hardware or software. For hardware it is the collection of equipment that makes up the computer. For software it refers to an integrated number of computer programs to perform predefined tasks.
TAPE	A liner magnetic storage device rolled onto a reel or cassette.
TELECOMMUNICATION SYSTEM	The devices and functions relating to transmission of data between the central processing system and remotely located users.
TERMINAL	A device, usually equipped with a CRT display and keyboard, used to send and receive information to and from a computer via a communication channel.
UTILITY PROGRAMS	Special programs usually supplied by the producer of the operating system. They perform general functions such as making back up copies of diskettes and copying files from tape to disk.
VALIDATION	The assurance, through testing, that hardware or software produces specified and predictable output for any given input.
WORD	One or more adjacent bytes conveniently considered as an entity. A word is usually one to four bytes long, depending on make of computer.
PROTOCOL	Agreed upon set of standards which allow

Return to: Page Top | Inspection Start